NPS-FX-13-002

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

NPS FIELD EXPERIMENTATION PROGRAM FOR SPECIAL OPERATIONS (FEPSO) TNT 13-2 REPORT

by

Dr. Raymond R. Buettner
LtCol. Carl Oros, USMC (Ret.)
Ramsey Meyer
Nelly Turley

April 2013

Approved for public release; distribution is unlimited.

Prepared for: **Naval Postgraduate School, Monterey, CA**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
30-04-2013	Technical Report	December 2012-April 2013

4. TITLE AND SUBTITLE
NPS Field Experimentation Program for Special Operations (FEPSO) TNT 13-2 Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. Raymond. R. Buettner, LtCol. Carl Oros, USMC (Ret.), Ramsey Meyer, Nelly Turley

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Naval Postgraduate School, Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-FX-13-002

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Postgraduate School, Monterey, CA 93943

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This analysis is broken up into two parts, event analysis of TNT 13-2 and insights derived from the experiments themselves. The former includes an event overview and statistics, including a look at trends in UAS participation. The later identifies trends in technological domains including: Tactical Mesh Networking and Multipath, Tactical Cellular Technology, Rapid Mission Planning and Virtual Rehearsals and Conducted Energy Clothing. Appendixes provide: the Request for Information (RFI), list of experiments and schedule, experiment descriptions and after action reports. With the exception of the appendix, this document reflects the opinions of the author and does not represent the official policy or position of the Naval Postgraduate School, the United States Navy, or any other government organization. The data in the appendices were provided by the participants and have only been edited for clarity.

15. SUBJECT TERMS
Field Experimentation, Naval Postgraduate School and the United States Special Operations Command's (USSOCOM), Special Operations Research and Development Acquisition Center (SORDAC), Avon Park Air Force Range, multi-institutional semi-structured learning environment, After Action Report, Tactical Mesh Networking and Multipath, Tactical Cellular Technology, Rapid Mission Planning and Virtual Rehearsals, Conducted Energy Clothing.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Carl Oros
Unclassified	Unclassified	Unclassified	UU	39	**19b. TELEPHONE NUMBER** (831)656-3554

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RDML Jan E. Tighe
Interim President

Douglas A. Hensler
Provost

The report entitled *"NPS Field Experimentation Program for Special Operations (FEPSO) TNT 13-2 Report"* was prepared for and funded by the Naval Postgraduate School.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Raymond R. Buettner Jr.
Associate Professor

LtCol. Carl Oros, USMC (Ret.)
Research Associate

Ramsey Meyer
Research Associate

Nelly Turley
Research Associate

Reviewed and Released by:

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

NPS Field Experimentation Program for Special Operations (FEPSO)
TNT 13-2 Report

Table of Contents

NPS Field Experimentation Program for Special Operations (FEPSO)
TNT 13-2 Report

April 2013

Dr. Raymond. R. Buettner, Dir. Field Experimentation
LtCol Carl Oros, USMC (Ret.), Research Associate & PhD candidate, Dept. of Information Sciences
Mr. Ramsey Meyer, Research Associate, Dept. of Information Sciences
Ms. Nelly Turley, Research Associate, Dept. of Information Sciences

I. Overview and Statistics

TNT 13-2 was conducted at Avon Park Air Force Range, FL from 26 Feb – 7 Mar 2013. 320 total attendees participated in this TNT. This number is not only consistent with the down-trend since TNT 11-4 (a record high) but participation was slightly lower than TNT 11-2 (Avon Pk) levels (see Fig. 1). Total industry participation has leveled out from its 11-4 decline but total USG participation has dropped to well below TNT 11/12-x levels (see Fig. 2).

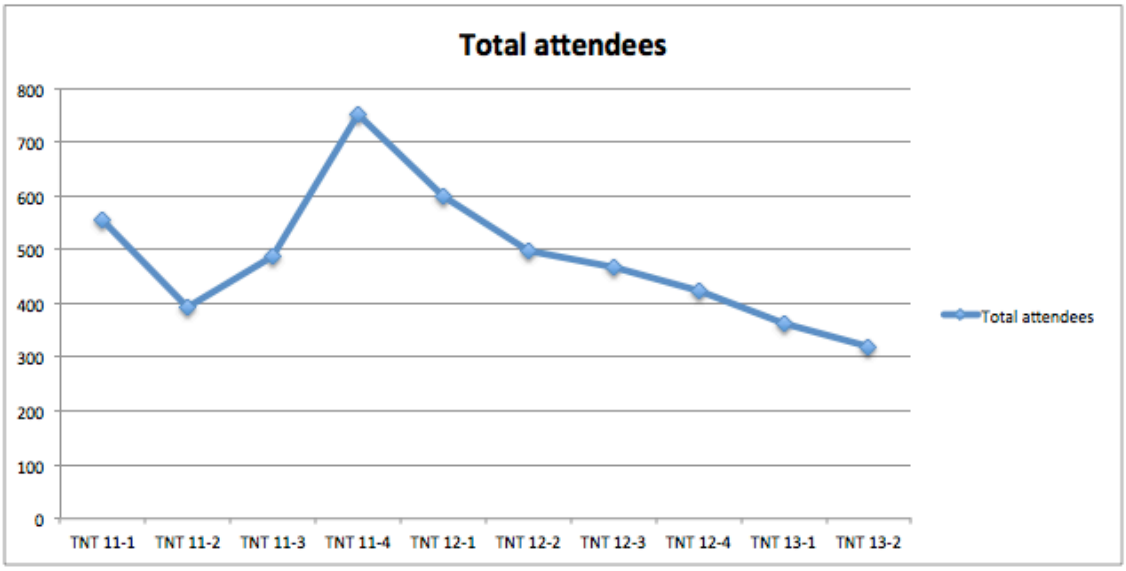

Figure 1. TNT total attendees (2011-2013/Q2)

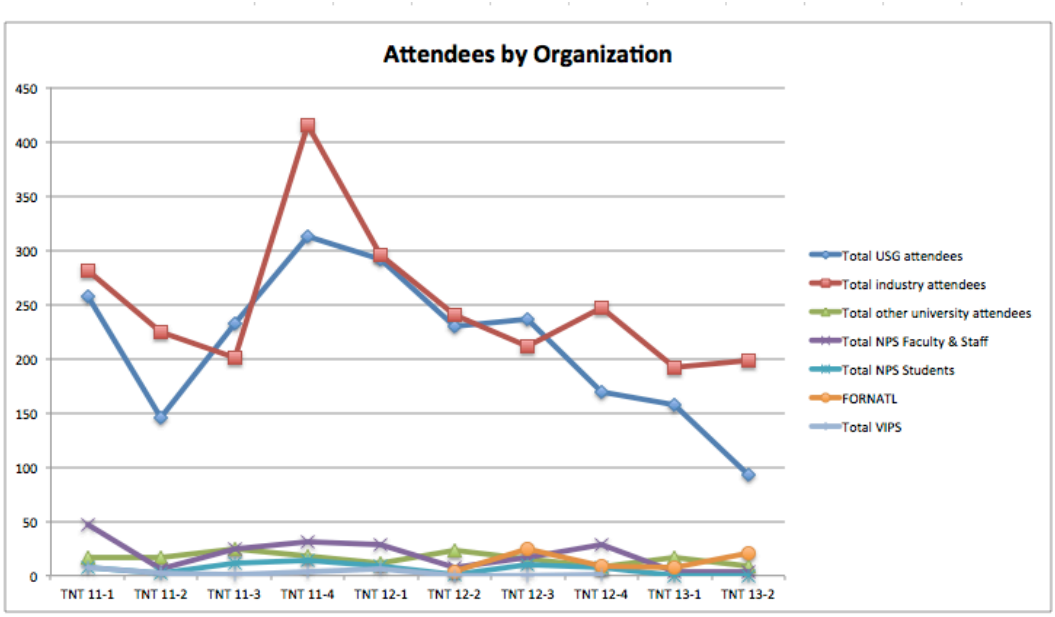

Figure 2. TNT attendees by organization (2011-2013/Q2)

Government lab (i.e., AFRL, NRL, ARL) participation in TNT has continued to decline to the lowest levels since 2011. In contrast, US Army Research, Development and Engineering Command (RDECOM) attendance--to include ARDEC, CERDEC, ERDEC, TARDEC, and AMREC—has been increasing (see Fig. 3).

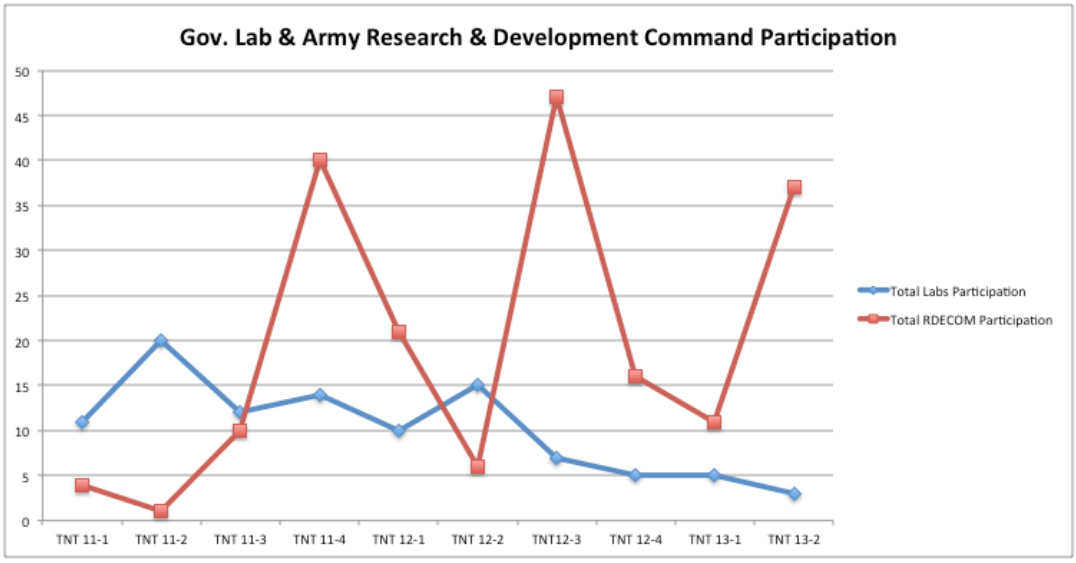

Figure 3. Comparison of Gov. labs vs. ARDEC TNT participation (2011-2013/Q2)

Figure 4 depicts the average TNT experiment Technology Readiness Level (TRL). The majority of technologies observed fall between TRL6 & TRL7.

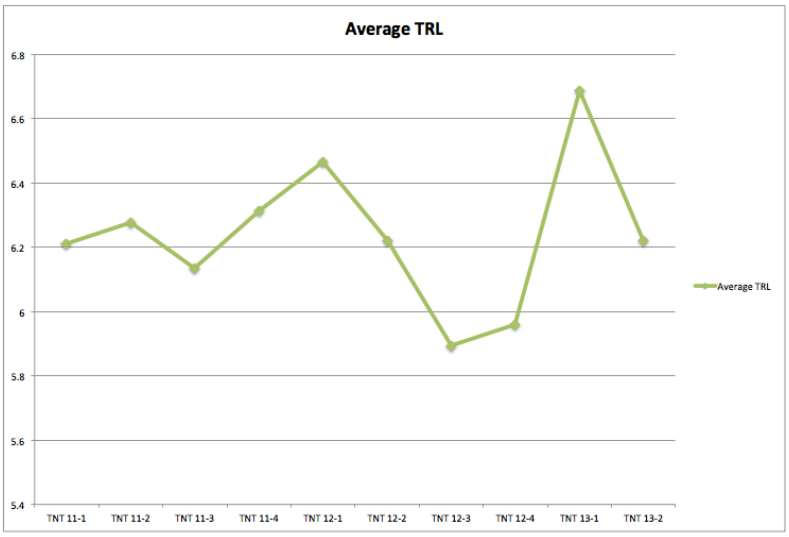

Figure 4. TNT TRL trend

The average number of experiments to date peaked in TNT 13-2 with 90 (see Fig. 5). This is a 125% increase over the historic average of 40 (2007-present). This increase in experiments has placed considerable demands on SORDAC S&T to now formally access vendor technologies and provide written feedback.

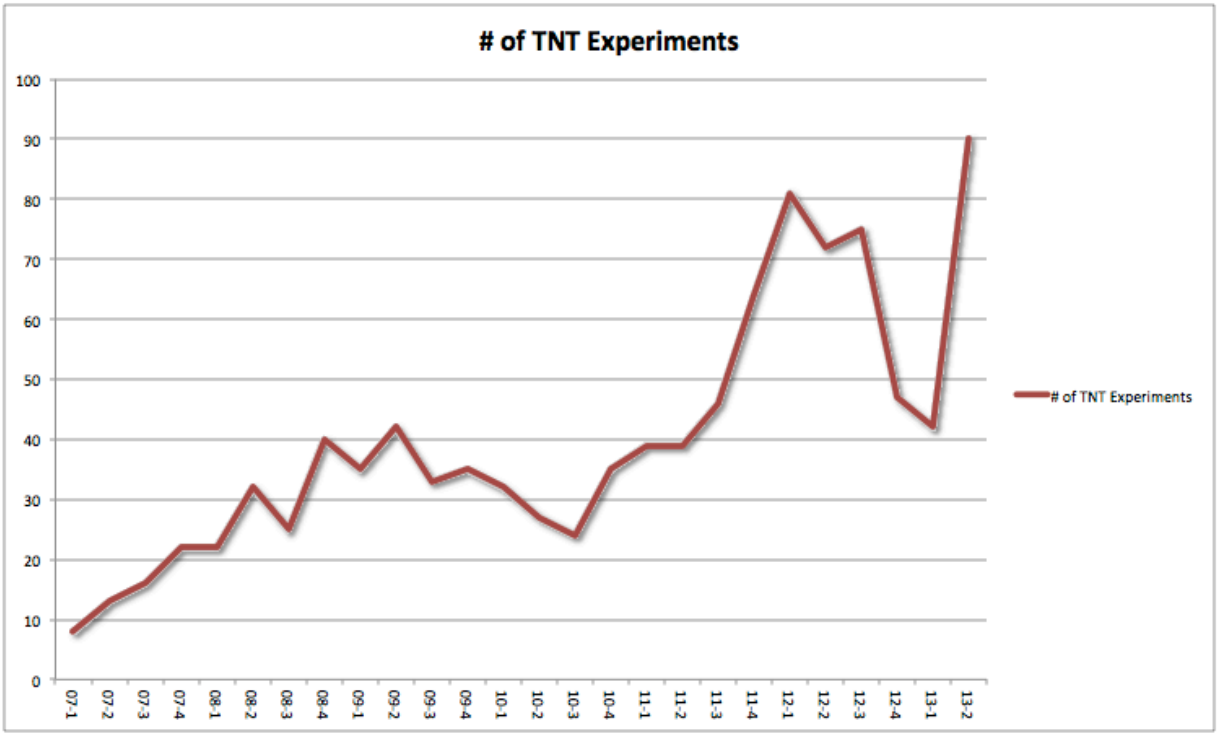

Figure 5. Number of TNT experiments (2007/Q4 - 2013/Q2)

*{*note: early 2007 and prior reflects low experiment numbers because many technologies were bundled into mission based experiments (MBE) and not recorded as single submissions}*

Figure 6 provides a breakdown of the number of experiments per mission category. The predominant technologies observed consistently fall within the C4 and ISR categories.

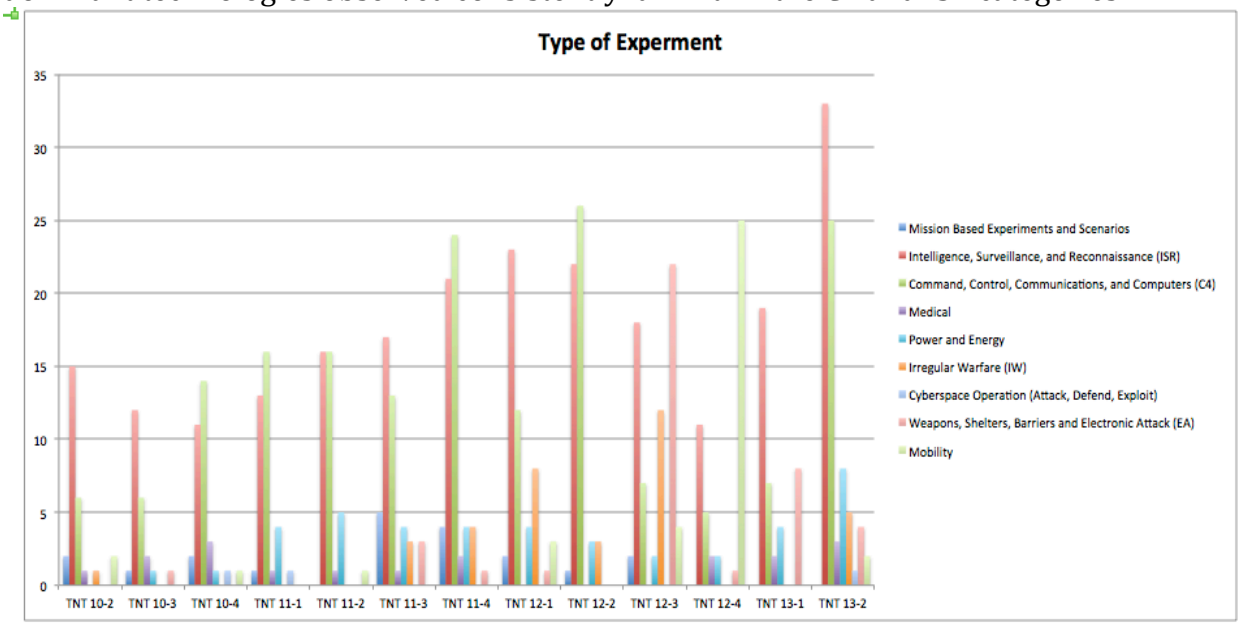

Figure 6. Breakdown of TNT experiment types (2011-2013/Q2)

A. Unmanned Autonomous System (UxS) Trends

Figure 7 depicts the trends in TNT unmanned autonomous systems (i.e, air, ground, surface, subsurface), or generically, "UxS" experiments since 2011. While non air types of UxS participation has been relatively stable, aerial vehicles have been in a steady decline; reaching an historic minimum during TNT 13-1 (zero). There have been many issues that have contributed to this decline. Since Naval Air Systems Command (NAVAIR) assumed oversight and responsibility for all NPS, U.S. Navy owned and operated aircraft, there have been challenges with ensuring compliance with Navy directives and more importantly, in continually applying for and receiving interim flight clearances (IFC) to operate in s timely and efficient manner. Failure to receive IFCs has led to a decline in NPS UAS TNT participation. TNT 13-1 held at Muscatatuck Urban Training Center (MUTC) also contributed to a lack of UAS participation, with only (1) helicopter UAS participating. This was due to the fact that the UTC does not operate under a restricted airspace. Rather, the UTC is within close proximity of a civilian airport and this requires a COA (certificate of authorization) from the FAA to operate there. No COA was in place to accommodate UAV participation in 13-1. MUTC and USSOCOM have since applied for a COA but it is unclear what types of aircraft will be permitted to fly directly over MUTC. Though the Jefferson Proving Ground (JPG) air-to-ground gunnery range is in close proximity to MUTC, UAVs would need to remain within the JPG range and if equipped with appropriate sensors, they may be able to have slant range only of MUTC. There are also other risks with flying UAVs at JPG that additionally may deter broader UAS participation. Much of JPG is restricted to ground traffic/foot traffic due to unexploded ordnance (UXO) hazards. UAS are confined to setting up and flying in a predefined location for safety reasons. Should a UAV crash/unintentionally land within the range complex or within an UXO area, only EOD

personal could attempt a recovery, and strictly that depends upon which area the aircraft landed. UAV participants would have to assume the risk of potentially losing an expensive vehicle because it could not be safely recovered.

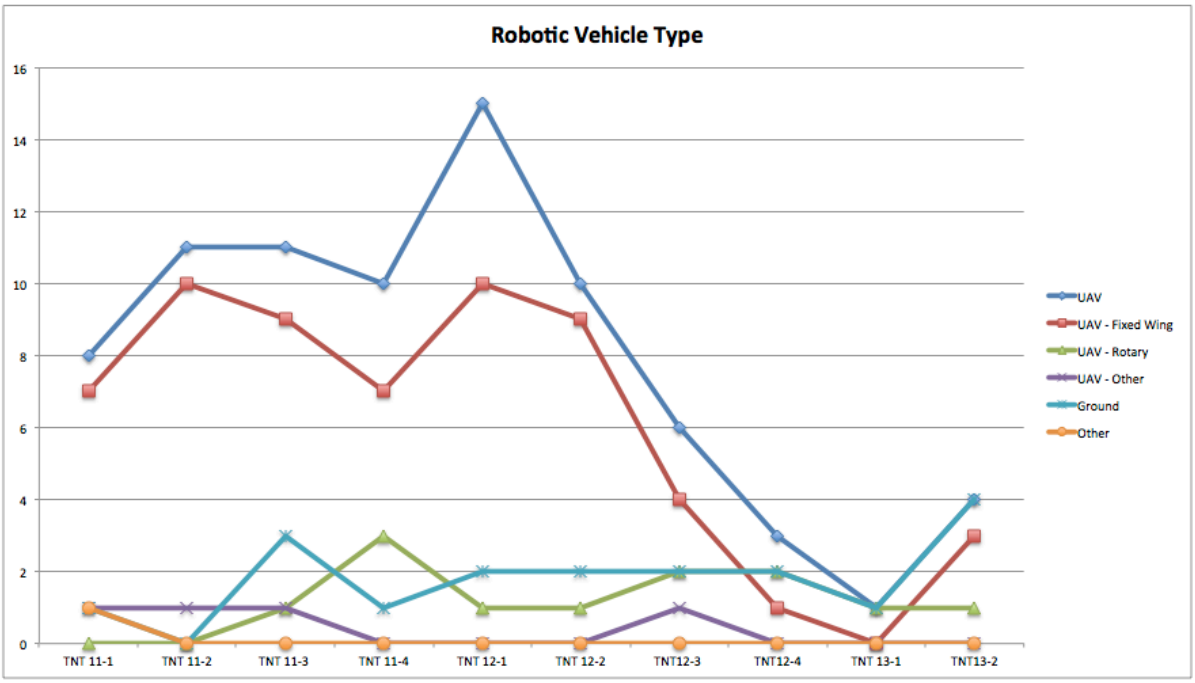

Figure 7. TNT UxS trends (2011-2013/Q2)

UAV sorties (Fig. 8) also reflect the decline described above.

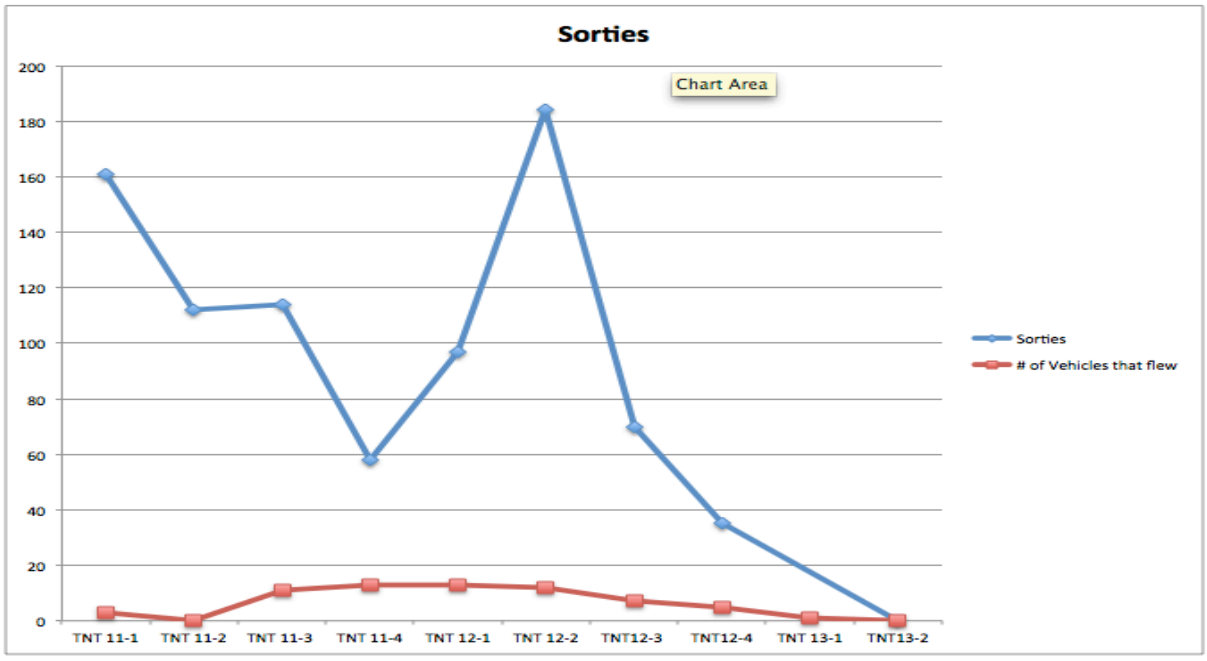

Figure 8. TNT UAV sorties (2011-2013/Q2)

II. High Level Technology Trends and Analysis

A. Tactical Mesh Networking and Multipath

Today, special operations have become increasingly dependent upon the network to delver timely, critical data to tactical users operating at the network's last tactical mile. These network technologies also must be sufficiently robust to operate in topographically extreme environments (i.e., non line of sight, dense urban, caves, tunnels, shipboard (above & below deck) and on aircraft). This requires these technologies operate with high availability in high multipath and potentially high Doppler environments. These networks also must have the ability to self-form and self-heal with without operator intervention. Trends in current tactical wireless networks have evolved from open standards, topologies with OSI layer three routing protocols to layer two self-forming-self healing peer-to-peer topologies. In this later group, we see emerging mesh technologies that are: (1) adaptive to high multipath environments through a combination of physical layer (PHY) and media access control layer (MAC) advancements and (2) have the ability to scale to 100's (+) nodes. We describe the TNT trends since 2002 below and recommend SORDAC S&T utilize these exemplar performance characteristics as discriminators when evaluating new tactical wireless technologies.

Since TNT began in 2002, tactical networking has evolved from early attempts to leverage and adapt commercial off the shelf (COTS) Institute of Electrical and Electronics Engineers (IEEE) open wireless networking family of standards (i.e., 802.11a,b,g,n and 802.16 d,e) to presently maturing peer-to-peer (P2P) mesh technologies (i.e. Persistent Systems "Wave Relay", Trellisware TW-220/230 with Tactical Scalable MANET (TSM) Waveform , and Harris' PRC-152A and 117G with Adaptive Networking Wideband Waveform (ANW2)) to name a few. Table 1 provides an historical sampling of the technology types (an associated vendors) and dates introduced and field tested at TNT.

In general, most all of the tactical networking technologies (including software defined "radios") demonstrated at TNT have been Open Systems Interconnect (OSI) layer one and two protocols. These network technologies can be further categorized according to their designed network topology (i.e. point-to-point (Pt-Pt), point-to-multipoint (Pt-MPt), or peer-to-peer (P2P) (mesh)). Today's most resilient mesh technologies observed incorporate design capabilities that permit robust communications in high multipath environments and can potential scale to 10s, 100s, or even thousands of nodes.

A.1 Point-to-point (Pt-Pt) and point-to-multipoint (Pt-MPt)

A variety of Pt-Pt and Pt-MPt networking technologies have been observed at TNT since FY02. Early technologies incorporated IEEE 802.11 variants with amplifiers and directional antennas to enhance range. These "wifi" protocols incorporate a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) (MAC) layer that is vulnerable to physical and

MAC layer denial of service attacks. Further, these open standards are vulnerable to off the shelf freeware "sniffing" and hacker tool kits. Encryption in these standards only focused on data encryption and not the MAC headers; leaving the frames exposed to traffic analysis and other exploits. All CSMA/CA devices are vulnerable to physical layer exploits regardless of encryption.

The PHY layer of these devices has also evolved over time; starting with direct sequence spread spectrum (DSSS) in 802.11, high rate direct sequence spread spectrum (HR-DSSS) in 802.11b, limited frequency hopping spread spectrum (FHSS) 802.11, to orthogonal frequency division multiplexing (OFDM) in 802.11 a,g,n , multiple input and multiple output (MIMO) in 802.11n, and proprietary wave forms (Harris ANW2 and Trellisware TSM) to name a few.

Redline introduced the first IEEE 802.16 variant (AN-50e) very early in the TNT program. This variant is more secure than the "WIMAX" open standard version (REDMAX today)as it incorporates X504 certificates and pseudo random connection IDs. The new versions in use are the AN-80i[1]. The Marine Corps was an early adopter of this high bandwidth technology and they employed HAIPE encryptors on the wireless links to provide Type I secure transmissions. Eventually Redline and Harris 802.16 products became part of the wireless point to point link (WPPL) program of record. Additionally, NPS created a 100 mile wireless Pt-Pt link with AN-50e's from Camp Roberts to Monterey, CA. BAE and Aeronix[2] also experimented in 2008/9 with radiation hardened versions (rack mount and miniaturized) of the 802.16 protocol in typical as well as enhanced mesh topologies. Aeronix's mini 802.16 EDL was also tested in Prioria's small UAV.

Table 1: Sampling of relevant network vendors, associated technologies and COTS products that emerged, were tested, or improved through TNT field experimentation FY02 to present.

Vendor + Associated	Network Technology	TNT Date(s) Introduced	Topology (s)*	Remarks
IEEE Standard, NPS	802.11a/b/g	2002	Pt-Pt | Pt-MPt	Early OSI Layer-1 & 2 networking standards explored in the field often with MANET (OSI Layer-3) routing protocols
BAE	802.16	TNT 08-1,2	Pt-Pt | Pt-MPt and Peer-to-Peer	BAE tested both enhanced 802.16 and mesh variants
GDC4S (General Dynamics C4 Systems)	Tactical Handheld radios	TNT 12-1	Peer-to-Peer	Introduced the Pathfinder mesh radio.
Harris	PRC-152 and 152(A)/117(G)	TNT 08-3,4; TNT 12-1,2,4;	Pt-Pt | Pt-MPt and Peer-to-	Explored SECNET 11 (secure 802.11); 802.16 (WPPL-D[3]); ANW2

[1] See: http://rdlcom.com/products/an-80i
[2] See: http://www.aeronix.com
[3] See: http://www.marcorsyscom.usmc.mil/sites/cins/Fact%20Books/NSC/SATCOM/2010%20WPPL-D%20(2)%20Fact%20Sheet.pdf

	with ANW2 mesh wave form	TNT 13-1	Peer	mesh wave form (PRC-152A + 117G) and tactical cellular (KnightLite/KnightHawk)
ITT / Motorola Mesh, Inter4, Sierra Nevada Corp, NPS	802.11 mesh variant	2003-2006	Peer-to-Peer	Explored ITT/Motorola mesh cards in lap tops and Sierra Nevada Corp. Tacticomps for SOCOM.
Redline , NPS	802.16 variant	2002- 2007	Pt-Pt | Pt-MPt	First reliable 802.16 variant produced. AS a result of TNT, USMC adopted Redline as part of WPPL-D POR. Used in NPS-Camp Roberts 100 mi. wireless network backbone.
Silvus	Mesh + MIMO	TNT 09-2,4 TNT 13-1	Peer-to-Peer	Started as crude prototype now marketing two military versions. Resilience to multipath using MIMO technology.
TrellisWare Tech., Inc. , NPS, MCWL, NSWC Dahlgren	CheetahNet. Mesh + Robust to multipath	TNT 08-4 TNT 09-1,2 TNT 10-1	Peer-to-Peer	Explored ground to ground; air to ground, and air-to-air mesh comms. And below deck (MIO). Resilient to multipath. Extensible to 1000s of nodes.
Persistent Systems (Wave Relay), NPS	High Bandwidth Mesh. 802.11 variant	TNT 08-1,2,3 TNT 09-1 & subsequent	Peer-to-Peer and traditional 802.11 topology	Hi bandwidth, reliable mesh network technology that TNT adopted as the test bed network and SOCOM has matured and supported to develop Suite-B encryption.

Pt-Pt: Point to point | Pt-MPt: Point to Multi-point | WIPPL-D: Wireless Point to Point Link version D | MIMO: Multiple Input Multiple Output | MIO: Maritime Interdiction Operations | OSI: Open System Interconnect | MANET: Mobile Ad-hoc Network

In summary, 802.16 emerged as a very reliable, high bandwidth capable link for stable, point to point/multi-point applications. It has not demonstrated reliable mesh performance to date (at least not at TNT). Presently, Wimax mobile (802.16m/e) and LTE (Long Term Evolution) standards have now been adopted by cellular carriers for 4G data communications. These cellular topologies, however, are still Pt-Pt/Pt-Mp topologies.

A.2 Peer-to-peer (mesh)

The predominant mesh technologies evaluated at TNT have been OSI layer two protocol devices. This is in contrast to MANET IP (OSI layer 3) protocols. Generally, network communication technologies that employ mesh algorithms at the data link layer are more responsive to physical and data link layer changes. Early TNT mesh networking attempts had no choice but to experiment with MANET protocols riding on top of 802.11 "Wifi" because no layer two devices existed. This early work was not successful do to the deficiencies in the 802.11 protocol as mentioned above. Work with USSOCOM at several early TNTs on Inter4's (now Sierra Nevada Corp.) Tacticomp[4] handheld mesh device resulted in replacing the Cisco 350 wireless card and layer three mesh algorithm with an

[4] See http://www.sncorp.com/prod/c4n/prodsheets/Tacticomp15.pdf. This device originated as a crypto fill device that who's chassis was redesigned to run Windows CE and a variety of applications. See also the Tacticomp v 5.0 tablet.

ITT/Motorola Mesh card[5] that was frequency shifted out of the 2.4 GHz UNII band. Since the protocol was proprietary it also could not be "sniffed." This technology was a modified 802.11 protocol and a CSMA/CA MAC layer.
In 2007-2008, Persistent Systems "Wave Relay" mesh products were introduced into the TNT testbed. This was the first high bandwidth, fairly robust mesh network to emerge with obvious tactical applications. TNT eventually adopted Wave Relay as the tactical mesh network backbone for TNT. Most air and ground assets were then finally able to connect to the tactical network. Several UAVs (Scan eagle, Raven, Rascal, Tern) utilize Wave Relay mesh for data communications. Wave relay has now produced Man Portable Units (MPUs) that incorporate VOIP and are Suite B encryption compliant. Wave Relay operates on top of the 802.11 protocol and thus employs a CSMA/CA MAC layer. The PHY layer is extensible to several frequency bands.

Trellisware's CheetahNet tactical mesh network device emerged in 2008. The TW-220 was a first generation device developed out of a research project sponsored by HQMC C4. Upon testing at NPS and during TNT, the Marine Corps Warfighting Lab (MCWL) selected the device for Company level and below operations and have experimented with mesh densities of up to 200 simultaneous users. The TW-220/230 are software defined radios that incorporate a proprietary TDMA MAC layer protocol. They are capable of simultaneous voice and data, separately software-encrypted to 256 AES. The CheetahNet radios utilize and iterative processing technique and a flooding (barrage) relay algorithm that increases the performance of the radio in high multipath (urban, caves, tunnels) and high Doppler environments. These devices hold potential to expand the network at the tactical level through fairly robust peer-to-peer networking. This technology has also been tested on air nodes as well.

Similarly, Silvus Technologies [6] network devices are focused on reliable mesh communications in high multipath environments as well. Silvus's approach, however, is achieved through MIMO (similar to 802.11n). Silvus first participated in TNT with a crude prototype in 2009 in order to gather field test data. Silvus recently demonstrated their SC3500 & SC3800 model radios at TNT 13-1 in Muscatatuck. These radios boast up to 65MBPS and 256 AES encryption and proved fairly reliable with air-ground comms in an ad hoc experiment.

Harris has also matured its PRC-152 and PRC-117G line of software defined tactical radios to accommodate its ANW2 wave form. This waveform is proprietary and believed to be TDMA in nature. The physical layer waveform is adaptive and this assists the device in applying its quality of service (QOS) algorithms for reliable voice and data communications. Though mesh capable, the ANW2 mesh network is not designed to support a network architecture comprised of every infantryman in a company or battalion. The optimal design is probably for one PRC-152 per squad at most, to serve as a data gateway. The challenge

[5] See: http://www.nothingfornow.com/websites/15-MeshNetworks_v4/pages/technology/technology_history.htm for a detailed historical overview of the DARPA/MEA networks to ITT/Motorola mesh technology development.
[6] See: http://www.silvustechnologies.com

for implementing PRC-152s at the company level is that each device requires the creation of its own network subnet. This is because every Harris radio that is Type I capable is also a router (layer 3) device and contains a HAIPE encryption module. This requires a well thought out network architecture and IP configuration management. These radios have not been tested in high multipath conditions to assess their performance.
The peer-to-peer mesh networking devices observed at TNT events have evolved from OSI layer 3 protocols operating on IEEE 802.11 variants to fairly mature OSI layer two 802.11 mesh (and PHY) modifications, to novel proprietary mesh waveforms that are now very resilient to high multipath and Doppler environmental effects. Assessing new technologies with regards to operations in these topographically extreme environments will prove to be a good discriminator. Configuration management and network management of these software defined radios can also be labor intensive. Hopefully we will see trends related to improved radio management software and network design and set up as well.

B. Tactical Cellular Technology

B.1. Trends and Advancement in Mobile Phones and Networks Statistics

Mobile phone technology has moved rapidly from basic voice-only devices to so-called "feature phones"—those that support other functions such as listening to music and basic web browsing—to smart phones, which contain more advances sensors (gyroscopes, accelerometers, GPS, compasses, light sensors, etc.), greater processing power, larger screens, more storage, and the ability to run third party applications. The shift to the more capable smartphone has led to rapid innovation and iteration of applications and uses for mobile technology. Since users have become comfortable using smartphones in their day-to-day activities, applying mobile phone technology to the battlefield represents a possible opportunity to reach new levels of connectivity and information generation and dissemination.

Generally speaking, experiments seen at FX events have transitioned from simple proof of concept of using mobile phone technologies in field environments to man portable mobile network base stations to securing the devices and network traffic. Some FX events have seen mobile phones used as sensors themselves, such as gamma radiation detectors.

B.2 Security of Devices & Communications

With the suggestion of widespread use of smartphones on the battlefield comes concern for the security of the devices and the communication links that serve them. A variety of technologies to secure the devices and the links have been proposed and developed at past Field Experimentation (FX) events. Since securing GSM or 2/3/4G networks beyond their built-in security features via fundamental lower layer technologies is difficult or essentially impossible, solutions to further secure mobile communications have focused on hardening the operating system and adding more secure software applications. (See Table 2.)

B.3 Mobile Networks and Backhauls

Mobile network experiments at past FX events have shown devices of various form factors capable of providing a mobile network for battlefield use. Devices have ranged from HMMWV-mounted antennae and equipment down to man portable units. Emphasis at recent FX events has been on smaller and smaller portable units, including many Pelican case-sized units.

More recent events have also focused on routing mobile phone networks over various network backhauls, such as ANW2, WiMAX, WiFi, etc. These technologies allow the mobile network to be extended beyond their normal range limits to include areas and other deployed units that could not otherwise be served by a given mobile network cell. Similarly, several recent events have also shown mobile network technologies designed to be carried aboard UAVs, thereby creating a mobile network with much greater coverage than can be attained via a terrestrial unit.

There have been no experiments dedicated to leveraging indigenous cell phone infrastructure for secure tactical comms.

B.4 Implications of technology

Mobile networks and devices have the potential to provide an unprecedented amount of information and situational awareness to both deployed units and command centers. The ability for all soldiers to carry a unit that provides voice, data comms, and Position and Location Information (PLI) has the potential to radically change battlefield dynamics. Those capabilities are further extended by the opportunity to use accessories that can either wired or wirelessly connect to mobile devices.

The introduction of mobile phone technology also has the potential to create new problems for soldiers—increased RF profile, radiating visible light, power requirements, more kit to carry, etc., all are challenges that must be addressed.

Table 2: Relevant mobile phone and network experiments, associated technologies that were tested, or improved through TNT field experimentation FY10 to present.

Vendor + Associated	Network Technology	TNT Date	Type of Exp.	Remarks
NPS Military Wireless Communications Group	GPRS, 802.11, PRC-117G	10-1	Hardware and software	Tested the feasibility of mounting pico cell technology in vehicles and using PRC-117G as backhaul; making calls via GPRS and sending data via WiFi.
Sahana	2G/3G	10-1	Software	Tested sending text messages from phones in simulated disaster environment to Sahana disaster management system
SSG Pacific	2G/3G	10-4	Hardware and software	Qualification of use of mobile phones in field environment.

NPS/MIT/WinTec/SVMH	2G	10-4	Hardware and software	Leverage 2G network connection for control of UAV.
Cummings Engineering Consultants	2G/3G	10-4	Software	Software suite to achieve Suite B certified end-to-end comms over mobile networks.
Western DataCom	2G/3G	11-1	Hardware and software	Ruggedized mobile network system run off of MIL-STD computer.
Harris	2G/3G	12-2	Hardware	Man portable tactical cellular system.
AT&T	3G/4G/LTE, 802.11 ad hoc	13-1	Smartphone app	Enables geocoded messages to be passed via mobile network or infrastructureless ad hoc WiFi.
Harris	3G/4G/LTE, ANW2 backhaul	13-1	Network hardware	Man portable and vehicle-mounted mobile network hardware
ID Rank Security	3G/4G/LTE, 802.11	13-1	Software and network hardware	FIPS-140-2 Level 1 compliant end-to-end encryption
PEO-C4	3G/4G/LTE, 802.11	13-1	Hardware and software	Extension of NIPRNET to mobile phones via SOF Deployable Node (SDN)
Advanced Ground Information Systems	2G/3G/4G, tactical radio backhaul	13-2	Software	Software creates bridge between mobile phone and tactical radios when connected via USB.
SRI International	2G/3G/4G	13-2	Software	Software app that compresses video and delivers over lower bandwidth connections.

C. Rapid Mission Planning and Virtual Rehearsals

Two novel approaches to mission planning were demonstrated at TNT 13-1 and 13-2 by General Atomics (GA) and Capturx/Adapx. Though these approaches and technologies, appear technologically diverse, when combined they represent a trend to leverage software to facilitate adaptive mission planning and ultimately realistic virtual rehearsals (i.e., GA). It is envisioned that future capabilities will enable planning and simulation updates in real time vice being restricted to the planning stage. An overview of the prospective technologies follows:

- *General Atomics* (Rapid Urban Planning with VBS2 Virtualization and SPIMAP terrain Generation) demonstrated their software at TNT 13-1. Their mission planning suite consisted of two applications: (1) a SMARTPlanner and (2) SPIMAP (Swift Point Imagery for Mission Awareness Planning). SMARTP allowed the creation of 3D virtual battlespace-2 (VBS2)[7] simulation missions from 2D SMARTPlanner missions. The SPIMAP terrain generation allowed terrain to be

[7] See: http://en.wikipedia.org/wiki/VBS2

generated from the latest imagery. This software demonstrated the ability to extract urban features out of 2D imagery and map data to generate a 3D model where users could insert mission objects (people, threats, etc.) into a battlespace simulation in order to dynamically rehearse actions on the objective and other mission profiles. Limiting the demo'd version was the inability to dynamically take in new imagery, process to the necessary format, and render in 3D. Only funding and development sponsorship have delayed productizing this type of capability.

- *Capturx/Adapx*[8] mission planning C2 software provides the ability through speaking and writing (digital pen) to create, store, disseminate and have access to structured data related to mission planning (e.g., military, first responders & potentially NGOs). Adapx also provides the capability for users to enter data via pen or voice on electronic or paper enhanced media (i.e., maps, forms, photos, etc.) that can also be geo-rectified.

These two examples represent a trend to quickly produce mission plans and virtual rehearsals from dynamic data sources. If the quality attributes of both of these approaches were merged, tactical operators would have a highly capable application suite that would allow for the ingest of emergent imagery and map data from which to simulate actions on the objective (COAs modeled and simulated with real intelligence threat data) and when satisfied produce an OPORD/FRAGO that documented the approved plan. The next leap would be tying Blue & Red PLI data into the system at run time to "observe" and manage the operations developments from a virtual reality perspective vice dependence upon eye-in-the-sky video feeds which may not be available due to platform and network constraints.

D. NO CONTACT LLC - Conducted Energy Clothing

No Contact LLC's Conducted Energy Clothing, developed by Adam Whiton and Yolita Nugent, is a wearable non-lethal weapon for protection in close quarters combat. Instead of a traditional hand held Taser, No Contact LLC has integrated an electro muscular disruption (EMD) delivery system into a light weight textile and integrated it into a jacket.[9] It delivers a high intensity, less than lethal, shock to the exterior of the jacket causing anyone in physical contact with it to instantly withdrawal. This allows the wearer to break free from a hold, prevent long-term contact, and lets them gain control of the situation. The product is aimed at civilian and military audiences, both of which face close quarters aggression. On the civilian side, its is aimed at women, stadium security, personal security details, law enforcement and correctional officers, all of for whom hand to hand assaults comprise the majority of attacks on their person.[10] Conductive Energy Clothing, unlike like

[8] See: http://c2.adapx.com and http://www.adapx.com

[9] There are further plans for gloves, working dog harnesses and working outerwear (White paper).
[10] See: http://www.no-contact.com/

most EMDs, does not require acts of aggression and cannot be taken away or used against the wearer.

The jacket contains an electrically conductive pathway that runs through the torso and arms and can be activated by the wearer. The jacket has four layers: outer shell, electrically conductive sub-layer, electrically insulative sub-layer, and liner. The outer shell is made of Teflon coated waterproof supplex nylon making it waterproof and allows it to function in the rain.[11] The electrically conductive sub-layer contains the electric pathway that produces the shock. The electrically insulative sub-layer, made of rubber or rubberized material, protects the wearer from the charge. The liner can be made of any suitable material.

To use the jacket, it is first armed; currently by a key, but it can be any coded switch that prevents unauthorized arming or disarming. This enables or disables power transmission between the power source and the electrically conductive pathway on the exterior of the jacket. When the jacket is armed it is on but not electrified.

The detachable power source is located in a rubber pocket on the inside of the jacket. The power source is capable of operating at from 20kV to 100kV.

To electrify the outer shell, the wearer squeezes or presses the palm pressure remotes in the cradle of each hand. This takes advantage of the natural tendency to clench fists in self-defense. This nearly hands free method of activation also prevents the remote from being dropped or taken away.

The trigger produces voltage differential between the two separated lines of the conductive pathway and launches an 80,000-volt low amp current thought the jacket.[12] The conductive pathway is pattered across the torso and arms, while avoiding areas such as the collar and underarms to prevent inadvertent shock to the wearer.[13] It can be formed from wire, wire mesh, electrically conductive textile, paint, conductive fiber or thread that can be woven, sewn, or printed, into the sub-layer. The high voltage can pass readily through any porous material up to about one inch thick, rendering even leather gloves ineffective.

Another layer of defense is the visual indicator. Located on the upper chest is a channel between the first and second conductive terminals in the exterior of the jacket, which creates an exposed electrical arc when armed or activated.[14] This demonstrates, both audibly and visually, the electrical charge on the jacket and can acts as a deterrent.

[11] See: http://www.no-contact.com/
[12] Potential refinements of the technology would comprise a dial or sensor in the activating switch that allows the wearer to adjust the level of charge produced on the jacket. See Patent: US6961227.
[13] There is also insulation around the zipper. See Patent: US6961227
[14] The visual indicator can be configured to be active when the jacket is armed or only when the wearer presses the activation switch.

D.1 Similar Work in Advanced Textiles and Personal Security clothing

With the decrease in price of microcontroller chips there has been in increase in inventors harnessing technology to solve social concerns.[15] Just like the mechanical products aimed to make the housewife's life easier in the 1950's, there is an increasing number of gadgets that set out to solve everyday annoyances such as barking dogs, to being able to display messages such as "Back Off!" on your rear windshield to ward off annoying drivers.[16] Some that are textile based include such as a t-shirt that acts like body armor by combining cotton with boron carbide (the same material that protects tanks)[17] to fabric that will monitor soldier's vitals[18] or trap poisonous gas.[19] Researchers in Berlin have created a smart fabric that is made of conductive threads connected to a microcontroller that can detect when it has been cut or ripped and triggers an alarm.[20] Other companies are looking at smart textiles that can store energy,[21] detect and produce sound,[22] alert a solider to the direction of an oncoming vehicle,[23] and gloves that turn hands into homing beacons.[24]

Similar to the Conducted Energy Clothing other researchers are developing hands free methods of disseminating electro muscular disruption (EMD), such as ArmStar, Blast Knuckles and SHE. Other researchers are developing devices that aim to specifically assist victims of abuse and unwanted contact. While not all offer protection from an attacker, they aim to increase a sense of security by allowing the wearer to be tracked and alert others to possible danger.

The ArmStar is a glove with a protective plate that extends over the forearm, which acts as a protective shield and can shock an opponent. Originally created to help defend the inventor against mountain lion attacks while mountain biking, he has developed it into a self-defense tool with an "aggregated technology deterrent." The technology deterrent contains not only the EMD but a flashlight and video camera for evidence.[25]
Blast Knuckles, commercially available, also take advantage of the body's natural tendency to clench fists and operates like plastic brass knuckles that shock the opponent on contact.[26]

Three Indian engineering students, two of who are females, have created a line of anti-rape undergarments that deliver a shock to attackers. The Society Harnessing Equipment (SHE) are undergarments that are still in prototyping phases but have already won a Gandhian

[15] See: "Revenge by Gadget" Wall Street Journal. http://online.wsj.com/article/SB118731374982900505.html
[16] See: "Revenge by Gadget" Wall Street Journal. http://online.wsj.com/article/SB118731374982900505.html
[17] See: University of South Carolina is designing http://www.sc.edu/news/newsarticle.php?nid=876#.UWhVRGR35ck
[18] See: http://www.ecouterre.com/u-s-military-develops-smart-undies-to-monitor-soldiers-vitals-during-combat
[19] See: http://www.news.cornell.edu/stories/2011/04/student-creates-clothes-trap-harmful-gases
[20] See: http://www.izm.fraunhofer.de/en/news_events/tech_news/a-smart-fabric-sets-off-the-alarm.html
[21] See: Fiber-Optic Solar Cell & Energy-Generating Fabrics: http://science.psu.edu/news-and-events/2012-news/Badding12-2012
[22] MIT Press Release: http://web.mit.edu/press/2010/hearing-fibers.html
[23] See: http://www.wired.com/gadgets/miscellaneous/news/2002/10/55764?currentPage=1
[24] Turns hands into Homing Beacons: http://www.helsinki.fi/news/archive/10-2012/11-16-00-51.html
[25] See: http://www.armstar.net/
[26] See: http://www.majorsurplus.com/Blast-Knuckles-Shocking-950000-Volts-P15011C2323.aspx

Young Technological Innovations Award.[27] The bra and underwear have sensors and produces an electric shock when contact greater than a hug is detected. They also have GPS and GMS capabilities to send a message to local police station, family or friend with the wearer's current location.[28]

The same team behind NO CONTACT is researching the use of fabric based pressure sensors with a wearable computer system that could detect and document physical abuse for MIT's Media Lab. The sensors distributed on the arms and chest of the wearer would categorize and measure the intensity of the patterns of abuse. It can detect: shaking, abusive contact and defensive injuries. The computer system would be able to record it over time to quantify abuse, provide evidence to authorities, or even just to the wearer to enable the process of self-realization of the abuse they have faced.[29]

Other wearable security accessories include GPS devices that are inconspicuous such as the Bodyguard Bracelet and Limmex Security Watch. The Bodyguard Bracelet is a fashionable bracelet with GSM and GPS technology that works as a personal alarm and tracking device. The bracelet is active when on the wrist, pulling the bracelet triggers the (silent) alarm, which sends a text message to up to three friends or a personal security service and activates live tracking. Your friends receive a text and can start tracking you on their phone. The PFO One works anywhere your cell phone works and requires purchase of a protection plan.[30]

The Limmex Security watch is advertised as the world's simplest and most attractive security system. Using GSM, a built in SIM, loudspeaker and microphone, it allows the wearer to make a call to emergency services (or another pre-determined phone number) by pushing the watch crown.[31]

[27] See: http://www.techpedia.in/award/upload/award_profile/she-society-harnessing-equipment-2013.pdf
[28] Currently looking to make the device more compact and looking to integrate it with Bluetooth to allow the pressure sensor to connect to the smartphone to send a message off immediately. See: http://www.techpedia.in/award/upload/award_profile/she-society-harnessing-equipment-2013.pdf
[29] See: http://web.media.mit.edu/~awhiton/ipv.htm
[30] See: http://pfoinc.com/how-it-works-pfo-protective-fashion-object.html
[31] Subscription required; currently only available in Switzerland and Germany. See: https://www.limmex.com/intl/en/function/overview

APPENDIX A: Request for Information (RFI)

Tactical Network Testbed (TNT) Collaboration Focus Area: Digital Soldier at Avon Park, FL

Solicitation Number: RFI-TNT-13-2_TNT_Experimentation
Agency: Other Defense Agencies
Office: U.S. Special Operations Command
Location: Headquarters Procurement Division

Original Synopsis
Nov 15, 2012
2:20 pm

Return To Opportunities List | Watch This Opportunity | Add Me To Interested Vendors

Solicitation Number:
RFI-TNT-13-2_TNT_Experimentation

Notice Type:
Special Notice

Synopsis:
Added: Nov 15, 2012 2:20 pm

A. INTRODUCTION: Tactical Network Testbed (TNT) Collaboration

This Request for Information (RFI) is NOT a solicitation for proposals, proposal abstracts, or quotations.
The purpose of this RFI is to solicit technology experimentation candidates from Research and Development (R&D) organizations, private industry, and academia for inclusion in future experimentation events coordinated by the U. S. Special Operations Command (USSOCOM) and the Naval Postgraduate School (NPS). USSOCOM invites industry, academia, individuals and Government labs to submit technology experimentation nominations addressing innovative technologies leading to possible Government/Industry collaboration for development of USSOCOM technology capabilities. The intent is to accelerate the delivery of innovative capabilities to the Special Operations Forces (SOF) warfighter.

SOF experimentation will explore emerging technologies, technical applications, and their potential to provide solutions to future SOF capabilities.
SOF experimentation focus areas for FY13 triannual TNT events are as follows:

- 30 Oct - 8 Nov 2012: Urban Operations at Muscatatuck UTC, IN
- 26 Feb - 7 Mar 2013: Digital Soldier at Avon Park, FL
- 18-27 Jun 2013: Signature Reduction at Camp Roberts, CA

Additional RFIs will be released to FedBizOpps approximately 75 days prior to each scheduled TNT event to provide additional details.

After review of the technology experimentation nomination submissions, the Government may invite select candidates to experiment their technologies at the USSOCOM & NPS sponsored TNT experimentation

ALL FILES

Vendor Loan Agreement Sample
Nov 15, 2012
Vendor_Loan_Agreemen...

GENERAL INFORMATION

Notice Type:
Special Notice

Posted Date:
November 15, 2012

Response Date:
Dec 17, 2012 4:00 am Eastern

Archiving Policy:
Automatic, 15 days after response date

Archive Date:
January 1, 2013

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
A -- Research & Development

NAICS Code:
541 -- Professional, Scientific, and Technical Services/541712 -- Research and Development in the Physical, Engineering, and Life Sciences (except Biotechnology)

event. The TNT venue will provide an opportunity for the submitter to interact with USSOCOM personnel for the purpose of USSOCOM assessing potential impact of emerging technology solutions on USSOCOM missions and capabilities. The intent is to accelerate the delivery of innovative capabilities to the Special Operations Forces (SOF) warfighter. Industry participation in experimentation activities does not suggest or imply that USSOCOM or NPS will procure or purchase equipment.

B. OBJECTIVE:

1. Background: USSOCOM conducts TNT experimentation events at Muscatatuck UTC, IN; at Avon Park, Fl, and in cooperation with NPS at Camp Roberts, CA. These cooperative TNT experiments are conducted with representatives from Government R&D organizations, academia, and private industry. TNT experimentation events provide an opportunity for technology developers to interact with operational personnel to determine how their technology development efforts and ideas may support or enhance SOF capability needs. The environment facilitates a collaborative working relationship between Government, academia, and industry to promote the identification and assessment of emerging and mature technologies for the primary goal of accelerating the delivery of technology discoveries to the SOF warfighter. The event facilitates SOCOM personnel to identify potential technology solutions, impacts, limitations, and utility to meet SOF technical objectives and thrust areas. Materiel solutions brought to the event should be at least Technology Readiness Level (TRL) of 3 but not greater than TRL 6. Experiments may be between a half day and five days in duration and be conducted in unimproved expeditionary-like conditions. At the discretion of USSOCOM, respondents may be asked to complete a vendor loan agreement (see attachment).

2. Experimentation Focus: Experiments will be conducted from 26 Feb 2013-07 Mar 2013, at Avon Park, FL and will explore emerging technology solutions and revolutionary improvements in technology for the individual Digital Soldier. Any technology-based experiment conducted at the event will need to be capable of supporting a SOF unit to provide a revolutionary improvement in SOF operations. Any and all solutions must include all necessary software and hardware to accomplish the mission. Digital Soldier technologies may include, but are not limited to:

• Situational Awareness (SA) to include combat ID and operations where GPS is not available
• Command, Control, Communications & Computers (C4) to include conformable & wearable antennae and wearable computers
• Improved Size, Weight and Power (SWaP) and Energy sources, to include wireless, or management devices
• Sensors including Intelligence, Surveillance & Reconnaissance (ISR), biomedical, physiological, etc.
• Medicine/Medical/Medic technology applications
• Human Performance
• Data Integration & Fusion (i.e. from the individual digital soldier to the weapon(s) system(s), the vehicle or other agnostic platform, C2 at multiple echelons, etc.)
• Individual soldier combat ready displays, including non-visual means of information display, and potentially utilization of cognitive thoughts and the surrounding environment to display personalized information
• Exoskeletons
• Ability to make revolutionary improvements in mobility, lethality, survivability and communications

Proposed solutions should take into consideration "lightening the load" of the operator, mentally and/or physically.

An exploratory closed cyber (virtual) network infrastructure, and an Electromagnetic Environment (EME) using electronic spectrum recording can be provided based on expressed interest. Please indicate in the Experiment Objectives Block of the white paper submission form, specific interest to conduct your experiment in either capability.

3. Security Requirements: Vendors should not submit classified information in the technology experimentation nominations.

4. Respondents interested in conducting experiments using technologies like: lasers, explosives, weapons using live fire, moving equipment, vehicles, and other technologies that present an occupational hazard shall prepare and submit a safety risk assessment. The risk assessment shall address the likelihood and severity of any inherent risks as well as risk mitigation measures required to bring the resultant risk to a low level. The risk assessment shall be submitted as an attachment to the experiment nomination. Reference MIL-STD-882D for instructions and information regarding risk assessments. Also, respondents are responsible for ammunition shipments to include an Interim Hazard Classification and coordination for receipt and storage at Avon Park, FL.

If your experiment will be radiating on a given frequency or frequency band, you must have prior approval to transmit on that frequency/frequency band. Prior approval may include compliance with Federal Communications Commission (FCC) Title 47, Part 15, a Special Temporary Authority (STA) from the FCC. If equipment is government owned and operating within a Federal Band, you must have National Telecommunications and Information Administration (NTIA) frequency approval. Your authority to radiate should be submitted along with your nomination, emailed directly to tech_exp@socom.mil, or presented on site during your equipment pre-check. The FCC recommends you submit your request at least 30 days prior to the start of the event.

5. Other Special Requirements: DO NOT SUBMIT PROPOSALS. SUBMIT TECHNOLOGY EXPERIMENTATION NOMINATIONS ONLY. EXPERIMENTATION NOMINATION SUBMITTALS FOR THIS RFI WILL ONLY BE ACCEPTED UNTIL THE CLOSING DATE OF 12/17/2012 1600 EST. No contracts will be awarded based solely on this announcement or any subsequent supplemental RFI announcements planned for FY13 TNT events.

C. SUBMISSION INSTRUCTIONS:

Technology Experimentation nominations shall be submitted electronically via USSOCOM webpage:
http://www.socom.mil/_layouts/FormServer.aspx?XsnLocation=/FormServerTemplates/whitepapersubmission.xsn . Multiple nominations addressing different technology experiments may be submitted by each respondent. Submissions will be reviewed by USSOCOM personnel to determine whether an experiment submission will be accepted for invitation. Each technology experiment nomination must address only one experiment.
Select respondents will be invited to participate in USSOCOM experiments. USSOCOM shall provide venues, supporting infrastructure, and assessment (operational and technical, based on availability of

resources and written request) personnel at no cost to invited respondent(s). Respondent's travel costs and technology experiments will be at the respondent's expense. The TNT venue will only provide basic access to training areas or ranges to conduct experiments, a facility to connect to the internet, basic venue infrastructure including frequency allocation/deconfliction, and portable power if needed. Invited respondents must be prepared to be self-sufficient during the execution of their experiments and not dependent on venue resources for success.

D. BASIS FOR SELECTION TO PARTICIPATE:

Selection of respondents to participate will be based on the extent to which the technology represents a particular class or level of capability that can be provided to Special Operations Forces.

Other considerations include:
- Technical maturity
- Relevance of or adaptability to military operations/missions
- Relevance to current operational needs
- Relevance to Event Focus Area

E. ADDITIONAL INFORMATION: All efforts shall be made to protect proprietary information that is clearly marked in writing. Lessons learned by USSOCOM from these experiments may be broadly disseminated but only within the Government. If selected for participation in TNT experimentation, vendors may be requested to provide additional information that will be used in preparation for the experiments.

F. USE OF INFORMATION: The purpose of this notice is to gain information leading to Government/Industry collaboration for development of USSOCOM technology capabilities and to assist in accelerating the delivery of these capabilities to the warrior. All proprietary information contained in the response shall be separately marked. Any proprietary information contained in response to this request will be properly protected from any unauthorized disclosure. The Government will not use proprietary information submitted from any one firm to establish future capability and requirements.

G. SPECIAL NOTICE: Respondent's attention is directed to the fact that Federally Funded Research and Development Centers (FFRDCs) or contractor consultant/advisors to the Government will review and provide support during evaluation of submittals. When appropriate, non-Government advisors may be used to objectively review a particular functional area and provide comments and recommendations to the Government. All advisors shall comply with procurement Integrity Laws and shall sign non-disclosure and rules of conduct/conflict of interest statements. The Government shall take into consideration requirements for avoiding conflicts of interest and ensure advisors comply with safeguarding proprietary data. Submission in response to this RFI constitutes approval to release the submittal to Government support contractors.

H. Per Federal Acquisition Regulation (FAR) 52.215-3 Request for Information or Solicitation for Planning Purposes (Oct 1997):

1. The Government does not intend to award a contract on the basis of this RFI notice or to otherwise pay for the information.

2. Although "proposal" and "respondent" are used in this RFI, your responses will be treated as information only. It shall not be used as a proposal.

3. In accordance with FAR Clause 52.209(c), the purpose of this RFI is to solicit technology experimentation candidates from R&D organizations, private industry, and academia for inclusion in future experimentation events coordinated by USSOCOM.

Contracting Office Address:
7701 Tampa Point Blvd
MacDill AFB, Florida 33621-5323
Primary Point of Contact:
TECH_EXP@socom.mil

Please consult the list of document viewers if you cannot open a file.

Vendor Loan Agreement Sample

Type: Other (Draft RFPs/RFIs, Responses to Questions, etc..)
Posted Date: November 15, 2012

Vendor_Loan_Agreement_15Nov12.doc (39.00 Kb)
Description: Vendor Loan Agreement

Contracting Office Address:
7701 Tampa Point Blvd
MacDill AFB, Florida 33621-5323

Place of Performance:
SEE RFI

United States

Primary Point of Contact.:
Geneva Emiliani,
Contract Specialist
geneva.emiliani@socom.mil
Phone: 8138266959

Secondary Point of Contact:
Christine E Johnson,
Contracting Officer
Christine.Johnson@socom.mil
Phone: 813-826-6038
Fax: 813-826-7504

Return To Opportunities List | Watch This Opportunity | Add Me To Interested Vendors

APPENDIX B: TNT 13-2 Experiment List & Schedule

Experiment List for TNT 13-2 Avon Park, FL: 26 Feb – 7 Mar 13:

A. Intelligence, Surveillance, and Reconnaissance (ISR):

649. Picatinny Optical Detection System (PODS) 2.1 – US ARMY RDECOM ARDEC

652. Sniper Detection & Visualization – HGH Infrared Systems, Inc.

655. Tactical Digital Holographic Wide Area Networked Display – Zebra Imaging

657. Image Acquisition & Exploitation Camera System (IAECS) – ACAGI

666. SWIR & SWIR/LWIR fusion systems & devices for the digital warrior – UTC Aerospace Systems

~~**676.** Video Share – Reconrobotics~~ - CANCELLED

679. A Remotely Operated Vehicle Capable of Identifying the Presence of Hazards to the Warfighter in Difficult Locations and Environments – Kromek

~~**683.** Out of band Fast Flashing Thermal IR Beacon – FLIR Systems~~ - CANCELLED

691. Soldier Centric Combat Ready Handheld Display Integrating New & Legacy Sensors – Digital Force Technologies

~~**692.** C-B4 – UTC Aerospace Systems~~ - CANCELLED

694. Advanced MicroObserver Unattended Ground Sensor System – Textron Defense Systems

695. Skyfire, Autonomous NL Alert-Sensing & Effects Node – US ARMY ARDEC

696. PEARL Infantry Gunfire Detection System – 01dB –Metravib

697. PILARw, M2 OTM Vehicle Mounted Gunfire Detection System with integration on Falconview – 01dB-Metravib

704. Buried Intrusion & Pursuit Alarm – Zybertec LLC

706. Improving Situational Awareness for the Special Operations Forces warfighter using Geo-Location in Full Motion Video – Churchill Navigation

709. Hyper Dynamic Range Optical Surveillance System – HyDROS – Phelps2020, Inc.

717. Thermal Matrix International IP-500 – Thermal Matrix International

718. Cobweb Force Protection & Area Denial System – Becatech Inc.

719. Improved SUAS ISR Capabilities using Onboard Video Processing Payloads – Innovative Automation Technologies, LLC

720. Salience Based Compression Video Transmission – SRI International

~~**721.** Performance Verification for Walleye Model 24S Millimeter Wave Surface Penetrating Imager – Walleye Technologies, Inc.~~ - CANCELLED

730. Detection of Powered & Unpowered Electronic Devices using Pulse Compression Harmonic Radar Techniques – L2 Integrated Solutions

732. Laser Gated Imaging (LGI) Hand-Held Camera – Elbit Systems of America

733. Networked Smart Collection (NSC) – ENSCO, Inc.

735. Multi-Shot Optical Surveillance System –MuSOS – Lentix

739. Bio-nanotags for Survivor Location & Identification, Tamper Detection, IFF & TTL – SRC (formerly Syracuse Research Corporation)

748. Stabilized Laser Designator – Sentech, LLC

753. Mission Command Technology Enabled Capabilities Suite – CERDEC

760. STERNA Non-Magnetic Precision Target Location System (PTLS) – Vectronix Inc.

762. Reco Roach – University of South Florida

~~**764.** ARES Multi-Mission UAS – Aurora Aerospace~~ - CANCELLED

765. A new generation body worn sensor network – Wireless Innovations, Inc.

766. Light Weight Back Pack Deployable Silent Propulsion Rotary Winged UAV – Jabriel, LLC

767. Enhanced Omni-Directional Multi-Configurable MBITR Antenna – Jabriel, LLC

768. Light Weight Multi-Hit Ceramic Composite Strike Plates – Jabriel, LLC

769. Improved Light Weight Transparent Armor – Jabriel, LLC

770. MAX 360 Real Time, fused multi-INT & Multi-Spectral Persistent ISR – L-3 KEO & MRT

~~**774.** 1.5 lb Counter UAV Radar – SpotterRF~~ - CANCELLED

B. Command, Control, Communications, and Computers (C4):

648. Airborne Web Services (AWS) – Fenwick Technologies

~~**659.** Spartan Dismount Squad Situation Awareness – Lockheed Martin MS2~~ - CANCELLED

660. NextGeneration PushToTalk & Messaging from Voxer – Voxer Federal LLC

~~**662.** RELIANCE Real-Time FMV Geo-Registration – Charles River Analytics~~ - CANCELLED

~~**667.** 13Mbps bi-directional antenna system – Mistral/ODF Optronics Ltd~~ - CANCELLED

~~**669.** Gesture Interface to Applications (GITA) – Battle Gear, LLC~~ - CANCELLED

674. Combined Small Unit Military Radio/Cellular Smartphone BFT Interoperability – Advanced Ground Information Systems

675. Geocast Based Situational Awareness – AT&T

684. A Field Experiment to Measure the Impact of a Tactile Communications Technology on Small Unit Situation Awareness, Detection Avoidance, & Navigation Efficiency - Collaborative Work Systems (CWS), Inc.

687. Provide Converged IP Services via Mobile Satellite Entry Point – Harris Corporation

688. Wide Area Cellular Communications – Harris Corporation

690. Rapid On The Fly Integration – Cervello Technologies

693. Indoor and GPS Denied Tracking & Location – TRX Systems, Inc

701. Mobile Soap – Mobile 4 carrier basestation – Georgia Tech Research Institute

705. Tactical MIMO Mesh Networking for the Digital Squad – Silvus Technologies

727. SAT>IP Digital Video/Data Dissemination-Wireless – SES Government Solutions

729. Co-Site Interference Cancellation – Communications, Electronics, Research and Development Engineer Center

731. Tactical Antennas for Comms, SATCOm and DF – MegaWave Corporation

~~**734.** Integrating ULTRA-Vis into a SOCOM tactical network – Applied Research Associates~~ - CANCELLED

~~**736.** ROBODEXS (Robotic Deployment & Extraction System) – US Army TARDEC~~ - CANCELLED

740. Beyond Line-Of-Sight Personal Communications – Battle Gear, LLC

741. Smart Radio Interface for US, NATO, Foreign Equipment – White Wolf Systems, LLC

745. Tactical Dismounted Intercom US, NATO, Foreign Equipment – White Wolf Systems, LLC

749. Tactical Audio Headsets with 3D Audio – Threat4 Tactical Audio Headsets

755. Tactical Coalition Command and Control Terminal (TC3T) – Salient Federal Solutions Inc.

758. Secure COTS Smartphone w/Mobile 3G Tower Demonstration – I.D. Rank Security, Inc.

759. MANET Mesh Network enhanced communications & MUOS BLOS w/route & retransmission capabilities – GDC4S

761. Vanguard Solution – ShadowTech Labs, Inc.

~~**763.** Distributed Tactical Fires – Department of Defense, Army~~ - CANCELLED

771. PEO-C4 Tactical Wireless Connectivity – USSOCOM

776. Linguistic Geometry Real-time Adversarial Intelligence and Decision-making (LG-RAID) – STILMAN Advanced Strategies; ARL-STTC

778. Natural Interface Technologies – Adapx Inc; ARL-STTC

C. Medical:

710. Flexible, printed electronics & demonstration (demo) of Wireless Sensor Integrated Conformal System (WiSIC) for Medical Triage – FlexTech Alliance & Physical Optics Corp.

~~**711.** Zephyr Technology Physiological Status Monitoring (PSM) – Zephyr~~ - CANCELLED

737. MTX Metalized Textiles – Versilant Nanotechnologies, LLC

777. Human Trauma Management in the Field – Adapx Inc; ARL-STTC

D. Power and Energy:

658. Turret Power Module & Spotlight Kit – US Army ARDEC

664. RENEWS – Army Power

671. Powerbelt – Zybertec LLC

673. 100 Watt Direct Methanol Fuel Cell Power System for powering end items & charging batteries – CERDEC, CP&I

680. Stand alone, right sized, 2kW flex fuel generator that is one man portable – CERDEC, CP&I

~~**703.** Idea/Title – Contour Energy Systems~~ - CANCELLED

728. Almost Real Time Electromagnetic Simulator (ARTEMS) – Space & Terrestrial Directorate, US Army CERDEC

738. Lightweight Warfighter Power Source – ARDICA Technologies Inc. w/ US Army/CERDEC/CP&I

751. Flexible PV Mats w/3X the Efficiency for Soldier Portable Recharing – Alta Device

~~**773.** Socom Referral 115 Weapon Mounted Electricity Generation from Recoil System – Don Riggs together with CWAS and University of Texas at Arlington~~ - CANCELLED

E. Irregular Warefare (IW):

681. SOF Technology Experimentation/Demonstration – Flight Test Aerospace, Inc. (FTA)

707. Wearable Electro-Muscular Disruption (EMD) Textile for Personal Protection – 10-20 Services, Inc.; No-Contact, LLC

743. Intelligence, Surveillance, & Reconnaissance Advanced Unmanned Systems – ProLogic, Inc.

747. UltraSocial – ProLogic, Inc.

752. Innovative Performance Solutions for Cognitive Readiness in SOF Operations – DSCI-Mesh Solutions

F. Cyberspace Operation (Attack, Defend, Exploit):

726. Digital Soldier Secure Information Fusion – Owl Computing Technologies, Inc.

G. Weapons, Shelters, Barriers and Electronic Attack (EA):

663. Nautilus Rotating Picitinny Rail – Azimuth Technology, LLC

698. BattleHawk Squad Level Loitering Munition – Textron Defense Systems

702. Covert Destruction of Large Metallic Targets (Project Angrist) – Dynetics, Inc.

712. Concealment and Suppression for Weapons – Defense Logistics Support, Inc.

H. Mobility:

650. Prowler Dermoskeleton (Exoskeleton)-Dismounted SOF-Digital Soldier/Avon Park – Revision Military

654. Portable Three-Dimensional (3D) Driver Vision Enhancer (DVE) System Demonstration – Tactical 3rd Dimension (T3D) Systems Corporation

I. Other:

665. Persistent Close Air Support (PCAS) – Rockwell Collins, Inc.

668. JTAC-Mobile – Rockwell Collins, Inc.

670. Networked Tactical Gateway (NTG) – Rockwell Collins, Inc.

672. Advanced Voice Response Translator (VRT) with Global Language Coverage for High-Noise Urban Operations – Integrated Wave Technologies, Inc.

~~**677.** Long Range Iris (LRI) – ARDEC & the CYLAB Biometrics Center at Carnegie Mellon University (CMU)~~ - CANCELLED

~~**682.** Soft Biometrics (SoftBio) – ARDEC & the CYLAB Biometrics Center at Carnegie Mellon University (CMU)~~ - CANCELLED

708. Remote SAASM 'Puck' Receiver (RSR) – Rockwell Collins, Inc.

713. Layered Color Changing from Electrochromic – Defense Logistics Support, Inc.

715. Wrapping UAV – Defense Logistics Support, Inc.

725. XM210 Infrared Ground Illumination Parachute Signal (Hand-Held Signal IR Illumination Round) – US Army ARDEC/METC/EMTWD/Pyrotechnics Technology & Prototyping Division RDAR-MEE-T

772. Wearable Light Based Identification System – Identlight Technologies

~~**775.** New bispectral obscurant and visual smoke grenades – US Army RDECOM/Edgewood Chemical Biological Center (ECBC)~~ - CANCELLED

Lunch Brief

Feb 28:

Aerogel is the world's lightest weight solid and best insulator, but it has not been practically useful until recently, because of its extreme fragility. Aspen Aerogels has developed a durable, flexible aerogel blanket insulation that is being used for industrial, aerospace, building and construction, and apparel and outdoor gear applications. Aspen's aerogel blankets provide exceptional thermal protection in a very thin package, saving significant weight and volume compared to conventional insulations. Aerogel has been used in numerous military applications including: insulating hot components in fixed and rotary wing aircraft (F-35, V-22, Apache, Kiowa); diver thermal protection; and tents, containers, and shelters. It can be utilized in new build systems or easily retrofit into most existing systems. Aerogels have also been used as electrical insulation in radar systems, eliminating significant decibel loss at high frequencies.

26 Feb - 1 Mar

*** Due to the exploratory nature of the TNT event, this schedule is advisory in nature and is subject to change***										
TNT 13-2 Schedule - Avon Park										
Monday	Tuesday		Wednesday		Thursday		Friday		Saturday	
25-Feb	26-Feb		27-Feb		28-Feb		1-Mar		2-Mar	
Morning Brief	8:00		7:30		7:30		7:30		7:30	
*****Experiments are ALL DAY events unless otherwise noted. Night Events are ALL DAY and continue into NIGHT*****										
	665	Rockwell Collins Inc.	665	Rockwell Collins Inc.	668	Rockwell Collins Inc.	668	Rockwell Collins Inc.		
	670	Rockwell Collins Inc.	670	Rockwell Collins Inc.	708	Rockwell Collins Inc.	708	Rockwell Collins Inc.		
	771	USSOCOM	771	USSOCOM	771	USSOCOM	771	USSOCOM		
	701	Georgia Tech Research Institute	701	Georgia Tech Research Institute	730	L2 Integrated Solutions	730	L2 Integrated Solutions		
	704	Zybertec	704	Zybertec	650	Revision	650	Revision		
	720	SRI International	720	SRI International	702	Dynetics	702	Dynetics		
	710	FlexTech Alliance & Physical Optics Corp	710	FlexTech Alliance & Physical Optics Corp	709 735	Phelps2020 & Lentix	709 735	Phelps2020 & Lentix		
	717	Thermal Matrix International	717	Thermal Matrix International	717	Thermal Matrix International	717	Thermal Matrix International		
	680	CERDEC, CP&I	680	CERDEC, CP&I	680	CERDEC, CP&I	680	CERDEC, CP&I		
	673	CERDEC, CP&I	673	CERDEC, CP&I	673	CERDEC, CP&I	673	CERDEC, CP&I		
	660	Voxer Federal	660	Voxer Federal	770	L-3 KEO & MRT	770	L-3 KEO & MRT		
	694	Textron Defense Systems	694	Textron Defense Systems	671	Zybertec	671	Zybertec		
	753	CERDEC	753	CERDEC	672	Integrated Wave Technologies	672	Integrated Wave Technologies		
	698	Textron Defense Systems	698	Textron Defense Systems	Lunch Brief 1200-1300		707	10-20 Services; No-Contact		
Travel Day	729	CERDEC	729	CERDEC	777	Adapx, Inc.	777	Adapx, Inc.		
	776	STILMAN	776	STILMAN	776	STILMAN	776	STILMAN		
	731	MegaWave	731	MegaWave	731	MegaWave	731	MegaWave		
	733	ENSCO Inc.	733	ENSCO Inc.	733	ENSCO Inc.	733	ENSCO Inc.		
	715 713	Defense Logistics Support	715 713	Defense Logistics Support	684	Collaborative Work Systems	684	Collaborative Work Systems		
	778	Adapx, Inc.	778	Adapx, Inc.	778	Adapx, Inc.	778	Adapx, Inc.		
	755	Salient Federal Solutions	755	Salient Federal Solutions	755	Salient Federal Solutions	755	Salient Federal Solutions		
	657	ACAGI	657	ACAGI	727	SES Government Solutions	727	SES Government Solutions		
			652	HGH	681	Flight Test Aerospace	681	Flight Test Aerospace		
			696 697	Metravib	712	Defense Logistics Support	712	Defense Logistics Support		
					695	US Army ARDEC	695	US Army ARDEC		
					707	10-20 Services; No-Contact				
					652	HGH				
					696 697	Metravib				
					657	ACAGI Night Ops				
Hot Wash		1700		1700		1700		1700		1700

Zone 1 - TOC
Zone 2
Zone 3
Zone 4
Echo Range
Oscar Range
Building 77

*** Due to the exploratory nature of the TNT event, this schedule is advisory in nature and is subject to change***

TNT 13-2 Schedule - Avon Park

Sunday		Monday		Tuesday		Wednesday		Thursday		Friday
3-Mar		4-Mar		5-Mar		6-Mar		7-Mar		8-Mar
Morning Brief		8:00		7:30		7:30		7:30		
*****Experiments are ALL DAY events unless otherwise noted. Night Events are ALL DAY and continue into NIGHT*****										
741 745	White Wolf Systems	741 745	White Wolf Systems	741 745	White Wolf Systems	741 745	White Wolf Systems	741 745	White Wolf Systems	
		688 687	Harris Corporation	688 687	Harris Corporation	688 687	Harris Corporation	688 687	Harris Corporation	
		663	Azimuth	663	Azimuth	740	Battle Gear	740	Battle Gear	
		758	I.D. Rank Security	758	I.D. Rank Security	758	I.D. Rank Security	758	I.D. Rank Security	
		747 743	ProLogic Inc.	747 743	ProLogic Inc.	728	Space & Terrestial, CERDEC	728	Space & Terrestial, CERDEC	
		752	DSCI-MESH Solutions	752	DSCI-MESH Solutions	690	Cervello Technologies	690	Cervello Technologies	
		765	Wireless Innovations	765	Wireless Innovations	705	Silvus Technologies	705	Silvus Technologies	
		718	Becatech	718	Becatech	726	Owl Computing Technologies	726	Owl Computing Technologies	
		674	Advanced Ground Information Systems	674	Advanced Ground Information Systems	762	USF	762	USF	
		738	ADRICA Technologies & US ARMY/CERDEC	738	ADRICA Technologies & US ARMY/CERDEC	691	Digital Force Tech	664	Army Power	
693	TRX Systems, Inc.	693	TRX Systems, Inc.	693	TRX Systems, Inc.	772	Indentlight Technologies Night Ops	751	Alta Device	
		759	GDC4S	759	GDC4S	751	Alta Device	737	Versilant Nontechnologies	
		648	Fenwick Technologies	648	Fenwick Technologies	737	Versilant Nontechnologies	749	Threat4 Tactical Audio Headsets	Travel Day
		655	Zebra Imaging	655	Zebra Imaging	749	Threat4 Tactical Audio			
		719	Innovative Automation Tech	719	Innovative Automation Tech	664	Army Power			
		676	Reconrobotics	676	Reconrobotics	654	T3D Night Ops			
691	Digital Force Tech	691	Digital Force Tech	691	Digital Force Tech	739	SRC Night Ops			
		706	Churchill Navigation	706	Churchill Navigation	766	Jabriel Night Ops			
		658	US Army ARDEC	658	US Army ARDEC	748	Sentech, LLC			
		761	ShadowTech Labs	761	ShadowTech Labs	768 769	Jabriel			
		767	Jabriel	767	Jabriel	649	RDECOM ARDEC Night Ops			
		675	AT&T	675	AT&T	666	UTC Aerospace Night Ops			
		650	Revision	650	Revision	732	Elbit Night Ops			
				679	Kromek	760	Vectronix Night Ops			
				772	Indentlight Technologies	725	ARDEC/METC/Pyro Night Ops			
Hot Wash		1700		1700		1700/Nite Ops/2200		17:00		

Zone 1 - TOC
Zone 2
Zone 3
Zone 4
Echo Range
Oscar Range
Building 77

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943

4. Raymond R. Buettner Jr. (2)
   Naval Postgraduate School
   Monterey, CA 93943